WHAT IS CLAIMED IS:

1. A method for rapid intrusion detection for network communication comprising the steps of:

receiving packets of network data in a network processor coupled to a network fabric;

forwarding routed network data to the network fabric; and

coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE and generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data.

2. The method of claim 1, further comprising the steps of:

storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected; and

storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures.

3. The method of claim 2, further comprising the steps of:

analyzing the packets of network data for validity thereby generating valid packets of network data as the selected data;

comparing the selected data to the store N intrusion signatures and generating, at network data speed, a pattern compare signal and particular ID data when a particular one of the N intrusion signatures is detected; and

executing the action code corresponding to the particular one of the N intrusion signatures detected.

4. The method of claim 3, wherein the PPDE comprises:

an input/output (I/O) interface for coupling data into and out of the PPDE;

M processing units (PUs), each of the M PUs having compare circuitry for comparing each of the sequence of input data to pattern data stored in each of the M PUs and generating a compare output, wherein an address pointer selecting the pattern data in each of the M PUs is modified in response to a logic state of the compare output and an operation code stored with the pattern data;

an input bus for coupling the sequence of input data to each of the M PUs in parallel;

an output bus coupled to the I/O interface for sending output data to the I/O interface;

control circuitry coupled to the I/O interface and coupling control data on a control data bus and identification (ID) on an ID bus to each of the M processing units; and

ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data, wherein the match ID and match data corresponding to the match ID are saved in a temporary register as the output data.

5. The method of claim 3, wherein the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs in response to the control data.

6. A system for rapid intrusion detection for a network communication comprising:

a network processor;

circuitry in the network processor for receiving network data from a network fabric;

circuitry in the network processor in the network processor for forwarding routed network data to the network fabric; and

circuitry for coupling the network processor to a parallel pattern detection engine (PPDE) for comparing in parallel selected data from the network data to M sequences of pattern data stored in the PPDE and generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data.

7. The system of claim 6 further comprising circuitry for storing N intrusion signatures in the M PUs sequence of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected.

8. The system of claim 6 further comprising circuitry for storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures.

9. The system of claim 6, further comprising:

circuitry for receiving packets of network data from the network fabric in the network process;

circuitry for analyzing the packets of network data for validity generating valid packets of network data;

circuitry for forwarding network data from the valid packets of network data to the PPDE,

circuitry for comparing the selected data to the store N intrusion signatures and generating, at network data speed, a pattern compare signal and particular ID data when a particular one of the N intrusion signatures is detected; and

circuitry for executing the action code corresponding to the particular one of the N intrusion signatures detected.

10. The system of claim 9, wherein the PPDE comprises:

an input/output (I/O) interface for coupling data into and out of the PPDE;

M processing units (PUs), each of the M PUs having compare circuitry for comparing each of the sequence of input data to a pattern data stored in each of the M PUs and generating a compare output, wherein an address pointer selecting the pattern byte in each of the M PUs is modified in response to a logic state of the compare output and an operation code stored with the pattern data ;

an input bus for coupling the sequence of input data to each of the M PUs in parallel;

an output bus coupled to the I/O interface for sending output data to the I/O interface;

control circuitry coupled to the I/O interface and coupling control data on a control data bus and identification (ID) on an ID bus to each of the M PUs; and

ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data, wherein the match ID and match data corresponding to the match ID are saved in a temporary register as the output data.

11. The system of claim 10, further comprising cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively

coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs in response to the control data.

12. The system of claim 11, wherein the PPDE further comprises an input buffer coupled to the I/O interface for receiving and writing input data as parallel data at a write address.

13. The system of claim 12, wherein the PPDE further comprises a multiplexer coupled to the input bus and the input buffer for sequentially coupling single data from the input buffer data to the input bus, wherein parallel data are selected using a read address.

14. The system of claim 13, wherein the PPDE further comprises an output buffer coupled to the output bus and to the temporary register for receiving and writing output data to the output buffer at a write address and coupling output data to the output bus corresponding to a read address.

15. The system of claim 10, wherein each of M PUs has an ID register for storing a unique ID sent from the control circuitry.

16. The system of claim 10, wherein each of M PUs has a control register for storing the match mode data, wherein the match mode data determines criteria for generating the match signal and the match data.

17. The system of claim 10, wherein each of the M PUs has a memory register array for storing a sequence of the pattern data and corresponding operation codes addressed by an address register indexed by the address pointer.

18. The system of claim 11, wherein the cascade circuitry enables the stored patterns of two or more M PUs to be chained together as a single pattern using the chain data.

19. The system of claim 18, wherein the chain data inhibits indexing the pointer of one PU until an adjacent PU coupled with the cascade circuitry has compared a last pattern data to input data.

20. The system of claim 10, wherein the compare circuitry in each of the M PUs completes a compare of input data to selected pattern data and generates a compare output and modifies the address pointer in the same cycle of a clock signal.

21. An intrusion detection system comprising;

a network processor having an input connection to a network fabric and an output connection to the network fabric; and

a parallel pattern detection engine (PPDE) coupled to the network processor, the PPDE for comparing selected from the network data, in parallel, to M sequences of intrusion signature data corresponding to M intrusion signatures stored in the PPDE and generating a match output signal when one of the M intrusion signatures is detected within the network data, wherein the network processor receives network input data, processes the network input data for forwarding as valid network output data, and couples the valid network output data to the PPDE for real-time detection of intrusion patterns within the valid network output data.